(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 588 339 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **93114917.3**

(51) Int. Cl.[5]: **G07F 7/10**, G06F 15/30

(22) Date of filing: **16.09.93**

(30) Priority: **18.09.92 JP 249293/92**
18.09.92 JP 249294/92
18.11.92 JP 308688/92
26.11.92 JP 317254/92
26.11.92 JP 317255/92

(43) Date of publication of application:
23.03.94 Bulletin 94/12

(84) Designated Contracting States:
DE FR GB

(71) Applicant: **NIPPON TELEGRAPH AND TELEPHONE CORPORATION**
1-6 Uchisaiwai-cho 1-chome
Chiyoda-ku
Tokyo(JP)

(72) Inventor: **Ishiguro, Ginya**
Gurin Haitsu 12-2-403,
580, Nagasawa
Yokosuka-shi, Kanagawa(JP)
Inventor: **Muta, Toshiyasu**
1927, Nagasawa
Yokosuka-shi, Kanagawa(JP)
Inventor: **Sakita, Kazutaka**
2-14-1-613, Kaneya
Yokosuka-shi, Kanagawa(JP)
Inventor: **Miyaguchi, Shoji**
5-20-19, Bessho,
Ninami-ku
Yokohama-shi, Kanagawa(JP)
Inventor: **Okamoto, Tatsuaki**
94-2-5-503, Nagasawa
Yokosuka-shi, Kanagawa(JP)
Inventor: **Fujioka, Atsushi**
B-305, 9-2-12, Sugita,
Isogo-ku
Yokohama-shi, Kanagawa(JP)

(74) Representative: **Hoffmann, Eckart**
Patentanwalt,
Blumbach & Partner,
Bahnhofstrasse 103
D-82166 Gräfelfing (DE)

(54) Method and apparatus for settlement of accounts by IC cards.

(57) An IC card (6) has a card information memory area wherein there are written a master public key nA, card secret keys pU and qU, a card public key nU, a card identification number IDU, and a first master digital signature SA1 for information including the card identification number. An IC card terminal (2a,2b) has terminal information memory area wherein there are written a master public key nA, terminal secret keys pT and qT, a terminal public key nT, a terminal identification number IDT, and a second master digital signature SA2 for information including the terminal identification number IDT. When inserted into the IC card terminal, the IC card sends thereto the data nU, IDU, and SA1. The IC card terminal verifies the digital signature SA1 by the master public key nA and, if it is valid, transmits the data nT, IDT and SA2 to the IC card. The IC card verifies the digital signature SA2 by the master public key nA and, if it is valid, transmits information corresponding to the current remainder value V to the IC card terminal. The IC card terminal makes a check to see if the received information corresponding to the remainder value V is appropriate, and if so, becomes enabled for providing a service.

EP 0 588 339 A2

validity of the first master digital signature SA1 through use of the master public key nA and the card identification number IDU received from the IC card;

a step wherein when the first master digital signature SA1 is valid, the IC card terminal transmits at least the terminal identification number IDT and the second master digital signature SA2 to the IC card;

a step wherein the IC card verifies the validity of the second master digital signature SA2 through use of the master public key nA and the terminal identification number IDT received from the IC card terminal; and

a step wherein when the second master digital signature SA2 is valid, the IC card terminal generating a value V corresponding to the charge for a service specified by the IC card after the service is provided.

In the method for the payment of charges by IC cards according to a second aspect of the present invention, the respective IC card has card information memory means wherein there are written, as card information, from a management center a card identification number IDU, a predetermined password setting number Ns, a second master digital signature SA2 for the password setting number Ns, a first master digital signature SA1 for information containing the card identification number IDU and the second master digital signature SA2 and an IC card terminal has terminal information memory means wherein there are written, as terminal information, from the management center a master public key nA for verifying the master digital signatures, terminal secret keys pT and qT for creating a terminal digital signature and a terminal public key nT for verifying the terminal digital signature. This method includes:

a step wherein the IC card transmits the card identification number IDU and the first and second master digital signatures SA1 and SA2 to the IC card terminal;

a step wherein the IC card terminal verifies the validity of the first master digital signature SA1 and, if it is valid, prompts the card user to input a password Nc' and transmits it to the IC card after it is input;

a step wherein the IC card matches the password Nc' received from the IC card terminal with the password Nc stored in the card information memory and, if they match, transmits an authentication signal to the IC card terminal; and

a step wherein upon receiving the authentication signal, the IC card terminal becomes enabled for providing a service, and after the service, the IC card terminal records information including a value V corresponding to the charge for the service rendered and the card identification number IDU received from the IC card, as usage/management information, in usage/management information memory means..

According to a third aspect of the present invention, the IC card includes:

card information memory means for recording a master public key nA for verifying a master digital signature SA created using master secret keys pA and qA, a card identification number IDU for specifying or identifying the IC card, card secret keys pU and qU for creating a digital signature, a card public key nU for verifying the digital signature, and a first master digital signature SA1 for information containing the card identification number IDU and the card public key nU, the first master digital signature SA1 being created using the master secret keys pA and qA;

means for transmitting the card identification number IDU, the card public key nU and the first master digital signature SA1 to the IC card terminal;

means which receives a terminal identification number IDT, a terminal public key nT and a second master digital signature SA2 from the IC card terminal, verifies the second master digital signal SA2 through use of the master public key nA recorded in the card information memory means and, if it is valid, transmits to the IC card terminal an authentication signal which enables it for providing a service; and

usage information memory means for recording usage information including the remaining value V' updated by subtracting using the charge for the service rendered.

According to a fourth aspect of the present invention, the IC card terminal includes:

memory means for recording a master public key nA for verifying a master digital signature SA created using master secret keys pA and qA, a terminal identification number IDT for identifying the IC card terminal, terminal secret keys pT and qT for creating a terminal digital signature, a terminal public key nT for verifying the terminal digital signature and a second master digital signature SA2 for information including the terminal identification number IDT and the terminal public key nT, the second master digital signature SA2 being created using the master secret keys pA and qA;

means for transmitting the terminal public key nT, the terminal identification number IDT and the second master digital signature SA2 to an IC card;

means which receives a card identification number IDU, a card public key nU and a first master digital signature SA1 from the IC card, verifies the first master digital signature through use of the master public key recorded in the memory means and, if it is valid, enables the IC card terminal for providing a service; and

making the payment of charges through use of an IC card according to the present invention. IC card terminals 2a, 2b, ... perform processing for the payment of charges for services rendered to an IC card 6. For example, when the IC card 6 is a prepaid telephone card, the IC card terminals 2a, 2b, ... provide service by telephone. The IC card terminals 2a, 2b, ..., when installed, are each connected via a communication network 3 to a management center 4 which sets and holds security information under its control. In the following description the IC card terminals will be indicated generally by a numeral 2 except when a particular one of them is intended. The IC card 6 has initial data written by the IC card dispenser 5 when it is issued, and security information necessary for the IC card 6 is provided from the management center 4. Incidentally, in the case where some functions of the management center 4 are mounted on a portable telephone terminal or the like so that they are brought to the place where the IC card terminal 2 is located, the IC card terminal 2 need not always be connected via the communication network 3 to the management center 4 when it is installed.

Fig. 2 illustrates an example of the internal configuration of the IC card terminal 2 and Fig. 3 an example of the internal configuration of the IC card 6. The IC card terminal 2 comprises an IC card reader/writer 11 which reads and writes the IC card 6 inserted thereinto, function buttons 12 as of a keyboard, a display 13, a telephone controller 14, a network interface 15 for processing communication via the communication network 3, a handset 16 and a speech circuit 17.

In the IC card 6 there are stored in a ROM 61 programs for IC card procedures, digital signature creating and verifying algorithms and so forth, and a CPU 63 controls the entire processing of the IC card while utilizing a RAM 62 as a work area and communicates with the IC card reader/writer 11 of the IC card terminal 2 via an I/O interface 65 and contacts 66.

Fig. 4A shows the process that is performed when the IC card terminal 2 is installed. The IC card terminal 2 receives from the management center 4 such pieces of terminal information as listed below when it is installed.

(1) Master public key nA for verifying a master digital signature of the management center 4;

(2) Terminal secret keys pT and qT for the IC card terminal 2 to create a digital signature;

(3) Terminal public key nT for verifying the digital signature of the IC card terminal 2;

(4) Terminal identification number IDT for identifying the IC card terminal 2; and

(5) Master digital signature SA(nT:*IDT) by the management center for the terminal public key nT and the terminal identification number IDT, where the symbol "*" represents concatenation--for example, 001*0101 = 0010101.

After receiving these pieces of information, the IC card terminal 2 verifies the validity of the master digital signature SA(nT*IDT) through use of the terminal public key nT, the terminal identificaion number IDT and the master public key nA, and if the master digital signature SA(nT*IDT) is valid, then the IC card terminal 2 records these pieces of information in a terminal information area $2M_1$ of a memory in the telephone controller 14. No description will be given of the method for verifying the digital signature, because it is disclosed in the afore-noted various digital signature schemes. As described previously, the verification of the digital signature S(M) generally calls for an unsigned full document M and a public key for verification use, but in the following description there are cases where a simplified description, "the digital signature is verified using the public key" or "digital signature is verified" is used.

Incidentally, the management center 4 has set therein its master secret keys pA and qA and has functions of creating a different terminal identification number IDT for each IC card terminal 2 and the terminal public key nT and the terminal secret keys pT and qT corresponding to the terminal identification number IDT.

It is preferable that the terminal secret keys pT and qT be recorded in the terminal information area $2M_1$ in the IC card terminal 2 which is not easily accessible from the outside, for example, in a RAM of a one-chip CPU or battery backup RAM of a construction wherein the power supply from the battery is cut off when the IC card terminal 2 is abused.

In Fig. 4B there is shown the process that is performed by the IC card dispenser 5 when it issues the IC card 6. The IC card 6 receives from the IC card dispenser 5 such pieces of card information listed below that need to be held in the IC card 6. These pieces of information are provided in advance from the management center 4 to the IC card dispenser 5.

(1) Master public key nA for verifying the master digital signature of the management center 4;

(2) Card secret keys pU and qU for the IC card 6 to create it digital signature;

(3) Card public key nU for verifying the digital signature of the IC card 6;

(4) Card identification number IDU for identifying the IC card 6;

(5) Master digital signature SA(nU*IDU) of the management center 4 for the card public key nU and the card identification number IDU.

After receiving these pieces of card information, the IC card 6 verifies the validity of the master digital signature SA(nU*IDU) through use of the

value V is 10 yen or more, the IC card terminal 2 provides a prompt on the display 13 for input of the telephone number of a subscriber to be called and originates a call as the user dials the number.

In the above, when any one of the digital signatures is found invalid through verification, the IC card terminal 2 stops processing at that point and ejects or returns the IC card 6 to the user.

After completion of the service or call, the telephone controller 14 of the IC card terminal 2 (a remaining value updating part 2D in Fig. 5B) subtracts the service charge v--prestored in the memory of the telephone controller 14 or transmitted from the communication network 3 or service center--from the remaining value V to obtain a new remaining value V', after which the telephone controller 14 creates, in its digital signature creating part 2B, a terminal digital signature ST(V"IDU) for the value V' and the card identification number IDU through use of the terminal private keys pT and qT. Then the IC card terminal 2 sends the value V' and the digital signature ST(V"IDU) to the IC card 6.

The IC card 6 verifies the received digital signature ST(V"IDU) by the public key nT in the verifying part 6A and, if it is valid, records the remaining value V' and the other pieces of information nT, IDT, SA(nT"IDT) and ST(V"IDU) received from the IC card terminal 2, as card usage information, in the usage information area $6M_2$ of the EEPROM 64, erasing the previous card usage information. That is, the card usage information in the usage information area $6M_2$ is updated as indicated by the arrow in Fig. 5.

It is also possible to employ a configuration in which in the case of updating the usage information area $6M_2$ in the EEPROM 64 of the IC card 6 with the current card usage information including the new remaining value V' received from the IC card terminal 2, the current remaining value V' is compared with the previous remaining value V in the usage information area $6M_2$ and if the latter is greater than the former, then the new remaining value V' is regarded as abnormal or invalid. When such an abnormality is detected, the usage information area $6M_2$ of the IC card 6 is not updated but instead a code representing the abnormality detection is written into the IC card 6 to prevent its further use. This ensures to prevent the remaining value of the IC card 6 from being raised by altering the IC card terminal 2. Upon completion of the updating of the usage information area $6M_2$, an authentication information (OK) representing it is sent to the IC card terminal 2.

In this embodiment, when either one of the digital signatures SA and ST is abnormal, the remaining value is not updated but instead the abnormal contents of the IC card are recorded in a code form.

Since the IC card 6 and the IC card terminal 2 transmit to and receive from each other their identification numbers appended with the master digital signature of the management center as mentioned above, even if the transmitted and received contents are falsified by altering the IC card 6 or IC card terminal 2, the abuse can be detected by the verification of the digital signature at the receiving side. Moreover, even if the contents of the IC card could be copied to another IC card using a stolen IC card terminal, the falsification of the master digital signature of the management center for the card identification number is so difficult that there is no choice but to copy it; hence, such a copy can be checked by acquiring data of the abused IC card.

In Fig. 6 there are shown procedures for providing increased security against wire tapping of communication between the IC card 6 and the IC card terminal 2 through use of random numbers in the procedure of sending the remaining value V' from the former to the latter.

When the IC card terminal 2 recognizes the validity of the IC card 6 inserted thereinto, by verifying the master digital signature SA(nU"IDU) received from the IC card 6 as described above with respect to Fig. 5, the IC card terminal 2 generates a random number R in a random generating part 2C (Fig. 5B) and sends it to the IC card 6 together with the pieces of information nT, IDT and SA(nT"IDT). The IC card 6 verifies the master digital signature SA(nT"IDT) by the master public key nA and the received pieces of information nT and IDT. When the master digital signature is valid, the IC card 6 generates a random number X in a random generating part 6C (Fig. 5A) and creates a digital signature SU(R"X"V) of the IC card 6 for the random number R, the random number X and the remaining value V by use of the card secret keys pU and qU and then sends the thus created digital signature to the IC card terminal 2 together with the random number X and the pieces of card usage information V, SA(V"IDU) and IDC read out of the usage information area $6M_2$.

The IC card terminal 2 checks the master digital signature SA(V"IDU) to ensure that the remaining value V was provided from a valid terminal (including an IC card dispenser) to the IC card 6. Furthermore, the IC card terminal 2 verifies the digital signature SU(R"X"V) through use of the received X, V, the card public key nU and the previously generated random number R to ensure that the remaining value V is one that was received from the valid IC card 6. Then the IC card terminal 2 permits the start of the service specified by the card user.

Upon completion of the service, the IC card terminal 2 generates a digital signature ST-

The key KU may be delivered from the management center 4 to the IC card dispenser 5 together with the pieces of data nA, IDU, ... when they are delivered as described previously with respect to Fig. 5B. After this, the transmission and reception of signals between the IC card 6 and the IC card dispenser 5 described previously in respect of Figs. 4B and 4C are performed by ciper communication using the key KU inherent to the card 6.

On the other hand, the transmission and reception of signals between the IC card terminal 2 and the IC card 6 shown in Figs. 5 and 6 are carried out by cipher communication using the common key KO.

In the case where the IC card dispenser 5 and the management center 4 are connected online as described previously with reference to Fig. 7, the transmission of the card identification number IDU from the IC card 6 to the management center 4 enables the latter to derive the key KU from the card identification number IDU by use of the master secret key KA; therefore, it is possible to provide increased security by using the encrypting key KU inherent to the card, in place of the common key KO, for writing the prepaid amount into the card or recharging it.

While the foregoing description has been given on the assumption that the IC card dispenser 5 and the management center 4 are located at different places, they may be formed as a unitary structure with each other, and it is also possible to enclose the IC card dispenser 5 and the IC card terminal 2 in the same housing. Moreover, in the cases of transmitting the terminal secret keys pT and qT from the management center 4 to the IC card terminal 2 and transmitting the card secret keys pU and qU from the IC card dispenser 5 to the IC card 6, security can be further increased by transmitting the keys together with the master digital signature of the management center 4 and by verifying the signature at the receiving side.

According to the embodiments of Figs. 5 and 6, since the IC card 6 and the IC card terminal 2 each transmit the identification number and the public key to the other together with the master digital signature of the management center 4, even if the contents of communication are falsified by, for example, forcing the IC card terminal 2 open, the falsification can be detected by verifying the master digital signature of the management center 4 at the receiving side. Furthermore, even if the contents of the IC card 6 could be copied to another IC card by a stolen IC card terminal, for instance, the falsification of the master digital signature of the management center 4 is so difficult that there is no choice but to copy it intact; therefore, the copy could be checked by acquiring data of the IC card used.

Besides, it is impossible to issue an IC card equivalent to a normal or valid one by altering a stolen IC card terminal or through use of a personal computer and an IC card reader unless the master secret key for generating the master digital signature of the management center, placed under strict supervision, is known. In addition, since the validity of the IC card and the IC card terminal is verified by the identification number appended with the master digital signature of the management center 4 as referred to above, the IC card terminal 2 does not need to inquire of the management center 4 about the validity of the IC card 6 prior to or during the service being rendered.

Turning next to Fig. 9, a description will be given of an embodiment of the invention improved from the Fig. 6 embodiment applied to the prepaid card system. As in the Fig. 6 embodiment, the IC card system, each IC card terminal and the IC card are basically identical in configuration with those shown in Figs. 1, 2 and 3, except that the IC card terminals 2a, 2b, ... each have a list of invalid IC card identification numbers IDU1, IDU2, ... prestored in a memory area $2M_2$ of its internal RAM as described later on. The invalid identification number list is written into the memory area $2M_2$ by a down load from the management center 4, for instance, when the IC card terminal 2 is installed, and thereafter the list is updated by the management center 4 as required.

Fig. 9 shows processing for the card user to receive his desired service at the IC card terminal 2b different from that 2a used previously. The pieces of information or data prestored in the card information area $6M_1$ of the EEPROM 64 of the IC card 6 and in the terminal information area $2M_1$ of the RAM in the telephone controller 14 of the IC card terminal 2b are the same as in the case of the Fig. 6 embodiment. In this case, however, symbols representing pieces of information or data inherent to the respective IC card terminals 2a and 2b will be identified by superscripts "a" and "b", respectively. In the usage information area $6M_2$ of the memory 64 of the IC card 6 there is retained the previous usage information, which includes the remaining value V', the terminal identification number IDT^a,the terminal public key nT^a, the random numbers R^a and X, the master digital signature SA-(nT^a, IDT^a) and the terminal digital signature ST-(R^a, X, V', IDT^a) received from the IC card terminal 2a used previously as described in connection with Fig. 6. The IC card terminal 2b has the aforementioned list of invalid card identification numbers IDU1, IDU2, ... in another area $2M_2$ of the memory.

When inserted into the IC card terminal 2b different from that used previously, the IC card 6 sends thereto the card identification number IDU,

can be held under the control of the management center 4.

While in the above the IC card 6 and the IC card terminal 2 are configured so that they have, in their card information areas $6M_1$ and terminal information area $2M_1$, the secret keys pU, qU and pT, qT for generating digital signatures and the public keys nU and nT for them, respectively, and transmit desired pieces of information together with the digital signatures, it is also possible to omit such a function to simplify the processing of the IC card system.

Also it is possible to omit either one of the random number R and X although security decreases. Conversely, by prestoring algorithms for encipherment of information to be transmitted and a common key for encipherment and decipherment in memories of the IC card 6 and the IC card terminal 2, the mutual communication between them can be made by cipher communication to provide further increased security.

As described above, according to the Fig. 9 embodiment, since particular card information numbers are registered in the card identification number list of the IC card terminal 2, it is possible to inhibit the use of IC cards of the registered card identification numbers. Furthermore, when the IC card 6 is used, at least the terminal identification number identifying the IC terminal used and the random number generated by at least one of the IC card 6 and the IC card terminal 2 are registered as previous information in the IC card 6 and when the IC card 6 is used next, at least the card identification number and usage/management information derived from the card identification number, the remaining value before updating and the previous information are registered and supervised in the management center as information for specifying the initial state of the IC card 6 only in the case of updating the remaining value information. When the card identification number and the usage/management information of the currently used IC card 6 match those already registered, the card identification number is registered as abnormal in the card identification number list of the IC card terminal 2, by which it is possible to inhibit further use of the IC card 6 of the same card identification number as that registered.

Referring next to Fig. 10, another embodiment of the present invention will be described as being applied to a prepaid card system.

Fig. 10 shows procedures for the payment of charges by the IC card 6 in an improved version of the Fig. 5 embodiment. As in the Fig. 5 embodiment, the IC card system, the IC card terminal 2 and the IC card 6 are basically identical in configuration with those depicted in Figs. 1, 2 and 3. In this instance, however, the IC card terminal 2 has in the ROM of the telephone controller a program which executes an algorithm for updating a time stamp as described later on. For example, the afore-noted FEAL can be used as the algorithm for updating the time stamp.

The initial value TS_0 of the time stamp TS_t may be recorded in a memory area $2M_4$ of the RAM in the telephone controller 14 after being received from the management center 4 via the communication network 3 when the IC card terminal 2 is installed; alternatively, it may also be preset in the memory area $2M_2$ of the RAM in the telephone controller 14 when the IC card terminal 2 is fabricated. Update information $\underline{t}$ is initialized to a "0", for instance, and it is incremented by 1 upon each updating the time stamp TS_t. In the RAM of the telephone controller 14 there is provided a terminal list area $2M_5$ for registering a list of terminal identification numbers IDT of stolen or similarly troubled IC card terminals, initial values TS_0 of the time stamp corresponding to them and the update information $\underline{t}$ at the time when each trouble was found.

In the configuration of Figs. 1 through 3, the terminal identification number IDT, the initial value TS_0 of the time stamp and the update information $\underline{t}$ set in each IC card terminal 2 are registered in the management center 4. The time stamp TS_t set in the respective IC card terminal 2 is independently updated by its internal timer from the initial value TS_0, for example, every day under a predetermined algorithm; namely, the time stamp is replaced with a new time stamp in a sequential order $[TS_0 \rightarrow TS_1 \rightarrow TS_2 \rightarrow \ldots TS_t \rightarrow \ldots]$, and thus the previous time stamps disappear one after another. The updating of the time stamp need not always be periodic but may also be periodic. Upon each updating of the time stamp, the number of updates (i.e. the update information or data) t is updated to $t+1$. Each time stamp TS_t and the update information t need only to correspond to each other, that is, the time stamp may be a mere symbol and need not be a quantity.

Upon updating the update information t, the IC card terminal 2 automatically calls the management center 4 and transmits thereto the terminal identification number and the renewed update information. The management center 4 replaces the received update information t for the preregistered update information t of the corresponding terminal identification number IDT. Incidentally, it is necessary to utilize, for updating the time stamp TS_t, an algorithm which generates the succeeding time stamp TS_{t+1} from the current time stamp TS_t under an encryption algorithm E using an encrypting key K, as exemplified in Fig. 11, to thereby prevent the previous time stamp from generation. The afore-noted algorithm FEAL, for instance, can be

$TS^j_0 \rightarrow TS^j_1 \rightarrow TS^j_2 \rightarrow \cdots \rightarrow TS^j_t$

(2) The IC card terminal 2b verifies the validity of the signature $ST^a(TS^a_t)$ by the time stamp TS^j_t obtained by the above calculation and the public key nT^a received from the IC card 6.

(3) When the digital signature is not valid, the IC card terminal 2b decides that the IC card 6 is abnormal or invalid and stops further processing, then ejecting or returning the IC card 6 to the user.

(4) When the digital signature is valid, the IC card terminal 2b compares update information t^j corresponding to the above-noted terminal identification number IDT^j in the troubled terminal list and the update information t^a received from the IC card 6.

(5) When $t^a \leq t^j$, the update information t^a is judged as update information generated before the pieces of data IDT^j,TS^j_0 and t^j were registered in the terminal list; that is, the IC card 6 is judged to be an IC card whose card usage information (terminal identification number IDT^j, update information t^j, public key nT^j and digitally-signed time stamp $ST^j(TS^j_t)$) in the usage information area $6M_2$ had been updated by a stolen IC card terminal 2j (not shown) of the identification number IDT^j before it was stolen. As the result of this, the IC card terminal 2b regards the IC card 6 as valid and performs the subsequent processing accordingly.

(6) When $t^a > t^j$, the update information t^a is judged as update information generated after the pieces of data IDT^j,TS^j_0 and t^j were registered in the troubled terminal list; that is, the IC card 6 is judged to be an IC card whose card usage information was updated by the IC card terminal 2j of the identification number IDT^j after it had been stolen. As the result of this, the IC card terminal 2b regards the IC card 6 as invalid and discontinues the process and ejects or detains the IC cards in the IC card terminal 2b.

Fig. 12 illustrates another embodiment of the invention which provides further increased security through use of random numbers in the Fig. 10 embodiment as in Fig. 6. In a ROM 61 of the IC card 6 there are recorded an algorithm for generating the digital signature and an algorithm for generating the random numbers. In the card information area $6M_1$ in the EEPROM 64 of the IC card 6 there are stored the information in the card information area $6M_1$ in Fig. 10, together with the card secret keys pU and qU and the public key nU for the verification of the digital signature. In this case, however, the master digital signature used is SA(IDU*nU). In the usage information area $6M_2$ in the EEPROM 64 there are held all pieces of card usage information received from the previously used IC card terminal 2a, that is, the terminal identification number IDT^a, the public key nT^a, the master digital signature $SA(nT^a*IDT^a)$ for them, the update information t^a, the random number R^a, the previously generated random number X, a first digital signature $ST^a(R^a*X*V*IDU) = S^a$ generated by the previously used IC card terminal 2a for the random numbers R^a and X, the remaining value V and the card identification number IDU, and a second digital signature $ST^a(TS^a_t*S^a)$ generated by the previously used IC card terminal 2a for the first digital signature S^a and the time stamp TS^a_t.

When inserted into the IC card reader/writer 11 of the IC card terminal 2b, the IC card 6 sends thereto the card identification number IDU, the public key nU and the master digital signature SA(IDU*nU) as in the case of Fig. 10, and the IC card terminal 2b verifies the master digital signature SA(IDU*nU) by the public key nU. When the master digital signature is valid, the IC card terminal 2b sends the terminal identification number IDT^b, the public key nT^b and the master digital signature $SA(IDT^b*nT^b)$ to the IC card 6. The IC card 6, in turn, verifies the master digital signature $SA(IDT^b*nT^b)$ and, if valid, sends to the IC card terminal 2b the pieces of data R^a, X, V, IDU, S^a, IDT^a, t^a, $SA(nT^a*IDT^a)$, nT^a and $ST^a(TS^a_t*S^a)$ which are the previous card usage information.

Then the IC card terminal 2b verifies the validity of the first digital signature S^a by the public key nT^a. When the signature S^a is valid, the IC card terminal 2b matches the received terminal identification number IDT^a with data in the troubled terminal list, and if the former does not match the latter, the IC card terminal 2b generates the random number R^b and sends it to the IC card 6. In response to this, the IC card 6 generates the random number X' and generates a digital signature $SU(R^b*X'*V)$ for the random numbers R^b and X' and the remaining value V by use of the secret keys pU and qU, then sends it to the IC card terminal 2b together with the random number X' and the card public key nU. The IC card terminal 2b, in turn, checks the validity of the received digital signature $SU(R^b*X'*V)$ by the public key nU also received from the IC card 6. When the digital signature is valid, the IC card terminal 2b displays the remaining value V on the display 13 and then provides a predetermined service. After completion of the service the IC card terminal 2b obtains the new remaining value V' and generates a first digital signature $ST^b(R^b*X'*V'*IDU) = S^b$ for the random numbers R^b and X', the remaining value V' and the card identification number IDU by use of the terminal secret keys pT^b and qT^b and, at the same time, generates a second digital signature $ST^b(TS^b_t*S^b)$ for the time stamp TS^b_t and the first digital signature S^b, thereafter sending them to the IC card 6 together with the new remaining value V' and the

card there are written, at the time of issuing the IC card 6 from the IC card dispenser 5, the identification number IDU for specifying the user, a password setting number Ns assigned to each user, a master digital signature SA(Ns) generated by the management center 4 for the password setting number Ns by use of a master key, and master digital signature SA(IDU*SA(Ns)) generated by the management center 4 for the identification number IDU and the master digital signature SA(Ns) by use of the master key. When these pieces of data are written, the validity of the password setting number Ns can be checked through verification of the master digital signature SA(Ns) by the public key nA.

In the terminal information area $2M_1$ of the RAM in the telephone controller 14 of the IC card terminal 2 there are prestored the master public key nA for verifying the master digital signatures created by use of the master key, the terminal secret keys pT and qT for generating the digital signature by the IC card terminal 2 and the terminal public key nT for verifying the digital signature created by the IC card terminal 2.

When inserted into the IC card reader/writer 11 of the IC card terminal 2, the IC card 6 sends thereto the identification number IDU, the master digital signature SA(Ns) and the digital signature SA(IDU*SA(Ns)). The IC card terminal 2 verifies, in turn, the digital signature SA(IDU*SA(Ns)) by the master public key nA to ensure the validity of the identification number IDU. If the identification IDU is judged to be invalid, then the IC card 6 is ejected or returned and the process is discontinued. When the identification number IDU is judged to be valid, a prompt for the "input of password" is displayed on the display 13. During the display of this prompt the input of a password is enabled and the selection of the password registration by pressing a particular one the function buttons 14 is made effective.

Upon selective pressing of the password registration command button among the function buttons 14, the IC card terminal 2 proceeds to the password registration process. The IC card terminal 2 sends a notice of the password registration to the IC card 6 to indicate thereto the start of the password registration process, while at the same time the IC card terminal 2 provides a display "ENTER IDENTIFICATION NUMBER" on the display 13 to urge the user to enter the identification number. Upon entering of the identification number IDU' by the user with pushbuttons, the IC card terminal 2 matches it with the identification number IDU previously received from the IC card 6 to check the validity of the identification number IDU' input by the user. When the both identification numbers do not match, the IC card terminal urges again the user to input the identification number. If the identification number IDU' does not match the previous one IDU even after being entered three times, for instance, the IC card terminal 2 judges that the IC card 6, discontinuing the process. When the identification numbers match, the IC card terminal 2 produces a display "ENTER PASSWORD SETTING NUMBER" on the display 13, prompting the user to enter the setting number.

Upon entering the setting number Ns' by the user with pushbuttons, the IC card terminal 2 sends the setting number Ns' to the IC card 6. The IC card 6 matches the currently received setting number Ns' with the setting number Ns prestored in the afore-mentioned memory to check the validity of the setting number Ns' entered by the user. If they not match, the IC card 6 sends a mismatch notice to the IC card terminal 2, which urges again the user to enter the setting number. In the event that the current setting number does not match the previous one even after being entered three time, for example, the IC card terminal 2 judges that the IC card 6 being used is abused and ejects it and discontinues the process. When the setting numbers match, the IC card 6 sends an authentication signal OK (a first authentication notice) to the IC card terminal 2. The IC card terminal 2 provides a display "ENTER PASSWORD" on the display 13, prompting the user to enter the password. Upon entering of the password Nc by the user with pushbottons, the IC card terminal 2 creates a digital signature ST(Nc) for the password Nc by use of the terminal secret keys pT and qT and sends the digital signature ST(Nc) and the terminal public key nT to the IC card 6 together with the password Nc. The IC card 6 verifies the digital signature ST(Nc) by the terminal public key nT to check the validity of the password Nc. When the password Nc is valid, it is recorded in the RAM 62. The IC card 6 becomes enabled for use only after the password Nc is thus registered therein.

While in the above the setting number Ns' is verified on the IC card 6, it can also be checked at the IC card terminal 2 if the setting number Ns is also sent to the IC card terminal 2 together with the card identification number IDU at the beginning. However, this procedure is not preferable from the viewpoint of security, because the setting number Ns--information that must be kept strictly secret--is transmitted from the IC card 6. Besides, in the case where the identification number or setting number, entered by pushbuttons, do not match the previous one even after being entered three time, the IC card 6 could be disabled for further use by writing thereinto to the effect that the IC card 6 is invalid or abused.

Fig. 14 is a diagram for explaining the process in which the user receives a service at the IC card terminal 2 through use of the IC card 6 which is a

random number X and creates the digital signature SU(R*X) for the random numbers R and X by use of the card secret keys pU and qU, thereafter sending the random number X and the card public key nU to the IC card terminal 2 together with the digital signature SU(R*X).

The IC card terminal 2 verifies the digital signature SU(R*X) by the card public key nU and judges that the IC card 6 and the password are both valid, and then the IC card terminal 2 provides on the display 13 an indication that the service specified by the user is possible and executes the service. Upon completion of the service, the IC card terminal 2 records the identification number identifying the user, the data of use D and the service charge V in the service information area $2M_6$ in its internal memory and then ejects the IC card 6, thus completing the process. As is the case with the Fig. 14 embodiment, the data in the service information area $2M_6$ is transmitted to the management center 4 periodically, or when the amount of data stored reaches a fixed value, or when the IC card terminal 2 is polled by the management center 4.

In the above, it is possible to deal with the loss of the IC card 6 or similar trouble, by adopting a system configuration in which the card identification number IDU for specifying the IC card 6 and the master digital signature SA(IDU) the master digital signature SA(IDU) and the IC card terminal 2 verifies the master digital signature SA(IDU) by the master public key to check the validity of the card identification number. In other words, when the user reports the loss of the IC card 6 to the management center 4, the latter registers the card identification number of that IC card 6 in a black list in the IC card terminal 2 by down load. The IC card terminal 2 matches the card identification number IDU with those in the black list when the IC card 6 is inserted thereinto. If the card identification number of the inserted IC card 6 matches any one of the identification numbers registered in the black list, then the IC card 6 can be inhibited from use.

With a system configuration in which date information is prestored in the EEPROM 64 of the IC card 6 and sent to the IC card terminal 2 together with the card identification number IDU when the IC card 6 is inserted thereinto and compared with a calender incorporated in the IC card terminal 2 to judge whether the IC card 6 can be used or not, it is possible to employ the IC card 6 as a card of a limited term of validity.

By storing algorithms for encryption of transmission data and common keys for encryption and decryption in both of the IC card 6 and the IC card terminal 2, the communication between them can be made as a cipher communication, providing increased security.

As will be seen from the above, in the case of employing the IC card 6 and the IC card terminal 2 in the embodiments of Figs. 13 through 16, the IC card 6 and the IC card terminal 2 mutually verify their validity and the validity of the user is verified by the IC card 6 through the IC card terminal 2--this eliminates the need of accessing the management center having a database concerning user information when receiving a service or setting a password, and hence permits easy system configuration. Since there is no need of accessing the management center, the verification time can be reduced and the operability of the system is increased. Moreover, since the identification number is verified on the basis of the digital signature created by use of the master key that is known to the management center alone, the digital signature could never be created using the identification number of another user, for example. Further, the password cannot be known from an IC card picked up and the identification number and the setting number are also unknown; hence, the password cannot be changed either. It is possible, therefore, to construct a system of excellent security.

Fig. 17 illustrates a modified form of the IC card system shown in Fig. 16. The IC card terminal 2 and the IC card 6 are identical in their internal construction with those depicted in Figs. 2 and 3. In the card information area $6M_1$ in the EEPROM 64 of the IC card 6 there are prestored, at the time of issuing the IC card 6, the secret keys pU and qU for the creation of its digital signature, the public key nU for verifying the digital signature, the IC card identification number IDU and the master digital signature SA(nU*IDU) of the management center 4 for the identification number IDU and the public key nU. The IC card 6 has the password Nc stored therein by the process described previously with respect to Fig. 15 or 17. The identification number IDU of the IC card 6 is prestored in the management center 4. The user inserts the IC card 6 into the IC card terminal 2 when to receive his desired service. After completion of the service, the management center 4 performs the charging process for the IC card 6 used.

When inserted into the IC card reader/writer 11 of the IC card terminal 2, the IC card 6 sends thereto the pieces of information nU, IDU and SA(nU*IDU). The IC card terminal 2 verifies the master digital signature SA(nU*IDU) by the master public key nA and, if it is valid, provides a guidance on the display 13 to prompt the user to enter the password Nc.

When the user enters the password Nc' by function buttons 12, the IC card terminal 2 sends the entered password Nc' and the random number R, generated by the IC card terminal 2, to the IC card 6. The IC card 6 matches the received pass-

key nA for verifying a master digital signature SA created by said management center by use of master keys pA and qA, card secret keys pU and qU for creating a digital signature by said IC card, a card public key nU for verifying said digital signature of said IC card, a card identification number IDU and a first master digital signature SA1 created by use of said master keys for information including said card identification number IDU, and an IC card terminal has terminal information memory means in which there are written from said management center said master public key nA, terminal secret keys pT and qT for creating a digital signature by said IC card terminal, a terminal public key nT for verifying said digital signature of said IC card terminal, a terminal identification number IDT and a second master digital signature SA2 created by use of said master keys pA and qA for information including said terminal identification number IDT, and wherein said IC card is issued from said management center via an IC card dispenser and used to receive a service at said IC card terminal and settle the charge therefor, said method comprising:

a step wherein said IC card transmits said card public key nU, said card identification number IDU and said first master digital signature SA1 to said IC card terminal;

a step wherein said IC card terminal verifies said first master digital signature SA1 and, if it is valid, transmits said terminal public key nT, said terminal identification number IDT and said second master digital signature to said IC card;

a step wherein said IC card verifies said second master digital signature SA2 and, if it is valid, transmits information corresponding to the current remaining value V to said IC card terminal;

a step wherein said IC card terminal makes a check to see if said information corresponding to said current remaining value V is appropriate and, if it is appropriate, becomes enabled for providing a service;

a step wherein, after completion of said service, said IC card terminal creates an updated remaining value V' and generates a terminal digital signature ST for information including said updated new remaining value and then transmits said terminal digital signature ST to said IC card together with said updated remaining value V'; and

a step wherein said IC card verifies said terminal digital signature ST.

2. The method of claim 1, wherein said step of transmitting said information corresponding to said current remaining value V of said IC card is a step wherein said IC card creates digital signature for information including said current remaining value V and transmits it to said IC card terminal together with said current remaining value V and said card public key nU, and said step of checking said remaining value by said IC card terminal is a step wherein said IC card terminal verifies said digital signature of said IC card and, if valid, becomes enabled for providing said service.

3. The method of claim 2, which includes a step wherein when it is verified at said IC card terminal that said first master digital signature SA1 is valid, said IC card terminal generates a random number R and transmits it to said IC card; and

wherein said step of creating said digital signature of said IC card is a step wherein when it is verified that said second master digital signature is valid, said IC card generates a random number X and creates a digital signature for information including said remaining value V and said random numbers R and X, as said digital signature SU for information including said remainder value V; and

wherein said step of creating said terminal digital signature of said IC card terminal is a step wherein said IC card terminal creates a digital signature for information including said updated remaining value V' and said random numbers R and X, as said digital signature ST for information including said updated remainder value V'.

4. The method of claim 1, wherein said IC card has usage information memory means, and which further includes a step wherein after completion of said service said IC card updates the contents of said usage information memory means with whole information received from said IC card terminal.

5. The method of claim 1, wherein said IC card terminal has usage/management memory means, and which further includes: a step wherein after completion of said service said IC card terminal generates usage/management information from information including at least said remaining value V and said card identification number IDU received from said IC card prior to the start of said service and writes said usage/management information into said usage/management memory means; and a step wherein said IC card terminal transmits

nal identification number in said database.

10. A method of creating an IC card, comprising:

a step wherein an IC card dispenser transmits, to said IC card, card information including: a master public key nA for verifying a master digital signature created by a management center; card secret keys pU and qU for creating a digital signature by said IC card; a card public key nU for verifying said digital signature of said IC card; a card identification number IDU; and a first master digital signature SA1 created by said management center for information including said card public key nU and the card identification number IDU;

a step wherein said IC card verifies said first master digital signature SA1 and, if valid, writes said card information into card information memory means;

a step wherein said IC card reads out said card public key nU, said card identification number IDU and said first master digital signature SA1 from said card information memory means and transmits then to IC said card dispenser;

a step wherein IC said card dispenser verifies said first master digital signature and, if valid, transmits, to said IC card, an amount value V created by said management center and a third master digital signature SA3 for information said value V and said card identification number IDU; and

a step wherein said IC card verifies said third master digital signature SA3 and, if valid, writes information including said value V and said third master digital signature SA3, as initial data of card usage information, into usage information memory means.

11. The method of claim 10, which further includes:

a step wherein said IC card dispenser verifies said first master digital signature SA1 and, if valid, generates and transmit a random number Y to said IC card;

a step wherein said IC card generates a random number X and creates a digital signature SU for information including said value V and said random numbers X and Y and then transmits said digital signature SU said IC card dispenser together with said random number X;

a step wherein said IC card dispenser verifies said digital signature SU and, if valid, transmits said random numbers X and Y, said value V and said card identification number IDU to said management center;

a step wherein said management center creates, as said master digital signature SA3, a digital signature for information including said random numbers X and Y, said value V and said card identification number IDU and transmits said digital signature to said IC card via said IC card dispenser; and

a step wherein said IC card writes said third master digital signature, as said card usage information, into said usage information memory means together with said value V and said random numbers X and Y.

12. The method of claim 10 or 11, wherein said IC card has prestored therein an encrypting key KU produced by said management center from said identification number IDU by use of a master key KA at the time of writing said card identification number IDU, and when receiving said card identification number IDU, said management center creates said encrypting key KU by use of said master key KA and transmits said encrypting key KU to said IC card dispenser, and wherein transmission and reception between said IC card, said management center and said IC card dispenser is conducted using said encrypting key.

13. A password registration method for an IC card, wherein said IC card has card information memory means wherein there are written, as card information, from a management center a card identification number IDU, a predetermined setting number Ns, a fourth master digital signature SA4 for said setting number Ns, and a fifth master digital signature SA5 for information including said card identification number IDU and said fourth master digital signature SA4, and wherein an IC card terminal has terminal information memory means wherein there are written, as terminal information, from said management center a master public key nA for verifying a master digital signature, terminal secret keys pT and qT for creating a digital signature by said IC card terminal and a terminal public key nT for verifying said terminal digital signature; said method comprising:

a step wherein said IC card transmits said card identification number IDU and said fourth and fifth master digital signatures SA4 and SA5 to said IC card terminal;

a step wherein said IC card terminal verifies said fifth master digital signature SA5 and, if valid, becomes enabled for password registration processing and transmits a setting number Ns' to said IC card when it is entered;

a step wherein said IC card transmits an authentication signal to said IC card terminal

nT;

means for verifying a first master digital signature SA1, received from an IC card, by said public key nA and for transmitting an authentication notice to said IC card when said first master digital signature SA1 is valid;

means whereby a digital signature Su of said IC card for information including an amount value V and a card identification number IDU, received from said IC card, is verified by a card public key nU and a service is initiated when said amount value V is valid and sufficiently large;

means whereby upon completion of said service, the charge for said service is subtracted from said amount value V to obtain a remainder value V' and a digital signature ST by said terminal key for information including the remaining value V' and said card identification number IDU; and

means for transmitting said digital signatures ST, said remaining value V', said second master digital signature SA2, said terminal public key nT and said terminal identification number IDT to said IC card.

18. An IC card comprising:

a memory wherein there are prestored a master public key nA, a card secret key pU and qU for the creation of a digital signature of said IC card, a card identification number IDU, a card public key nU for verifying said digital signature of said IC card, a first master digital signature SA1 by said master key for information including said identification number IDU and said card public key nU, amount value information V, and a third master digital signature SA3 by said master key for information including said amount value information V and said card identification number IDU;

means which transmits said public key nU, said card identification number IDU and said first master digital signature SA1 to said IC card terminal upon insertion thereinto of said IC card.

means for creating a digital signature SU by said card secret key for information including said amount value information V;

means for transmitting said amount value information V and said digital signature SU to said IC card terminal upon receiving an anthentication notice from said IC card terminal; and

means for verifying received second master digital signatures SA2 and ST by said public keys nA and nT, respectively, and stores amount value information V' in said memory when said second master digital signatures SA2 and ST are valid.

19. An IC card terminal comprising:

a memory having stored therein a terminal identification number for specifying said IC card terminal;

a memory for storing card identification numbers as a card identification number list;

means for matching the card identification number received from an IC card with data in said identification number list and for initiating a service if amount value information received from said IC card is sufficient when said card identification number received from said IC card does not any one said card identification numbers in said list;

means for transmitting said terminal identification number to said IC card together with new amount value information after completion of said service;

means whereby only in the case of transmitting said new amount value information to said IC card, usage/management information is created from previous usage information including amount value information, the card identification number and the terminal identification number, received from said IC card prior to the start of said service;

means for transmitting said usage/management information to a management center together with said card identification number; and

means whereby card identification numbers received from said management center are additionally registered in said card identification number list.

20. An IC prepaid card system comprising:

an IC card including: usage information memory means for storing a card identification number identifying said IC card and previous usage information including amount value information; means for said card identification number, said amount value information and said previous usage information to an IC card terminal; and means for receiving new amount value information and usage information including a terminal identification number from said IC card terminal and for storing them in said usage information memory means;

said IC card terminal of claim 19; and

a management center which has a database for storing usage/management information for each IC card identification number and means whereby the card identification number and usage/management information received from said IC card terminal are matched with card identification numbers and

25. An IC card terminal comprising:

a memory wherein there are stored a master public key nA and a terminal public key nT for verifying a digital signature SA and terminal secret keys pT and qT for creating a terminal digital signature;

means which verifies a digital signature SA received from an IC card, by said public key nA and, if an identification number IDU received from said IC card is valid, enables the registration or entering of a password;

means whereby when the registration of a password is chosen, an identification number IDU' entered from input means is matched with said identification number IDU received from said IC card and when they match, the input of password setting number is instructed;

means for transmitting to said IC card a password setting number Ns' entered from said input means;

means which, when having received a first authentication notice from said IC card, creates a digital signature ST by said terminal secret keys pT and qT for information including a password Nc entered from said input means;

means for transmitting said password Nc, said digital signature ST and said terminal public key nT to said IC card;

means which, when the input of a password is chosen, transmits a password Nc' entered from said input means to said IC card; and

means for permitting a service when having received a second authentication notice from said IC card.

26. An IC card system comprising:

an IC card including: means for generating a random number X; means for creating an IC card digital signature SU1 for information including a random number R received from an IC card terminal and said random number R: means whereby a master digital signature SA created by a management center for information including a public key nU of said IC card and a card identification IDU, said random number said digital signature SUI, said public key nU and said card identification number IDU are transmitted to said IC card terminal; means for creating a IC card digital signature SU2 for information including service information M including a service charge, received from said IC card terminal, and said card identification number IDU; and means for transmitting said digital signature SU2 to said IC card terminal; and

an IC card terminal which has means for receiving and verifying said digital signatures SU1 and SA, means for creating and transmitting said service information M to said IC card, and means for receiving said digital signature SU2.

27. The IC card system of claim 26, wherein said IC card terminal includes means whereby a password Nc entered by a user is transmitted to said IC card, and said IC card includes means whereby said password Nc' received from said IC card terminal is matched with a password Nc prestored in a memory to thereby verify said password Nc.

FIG. 2

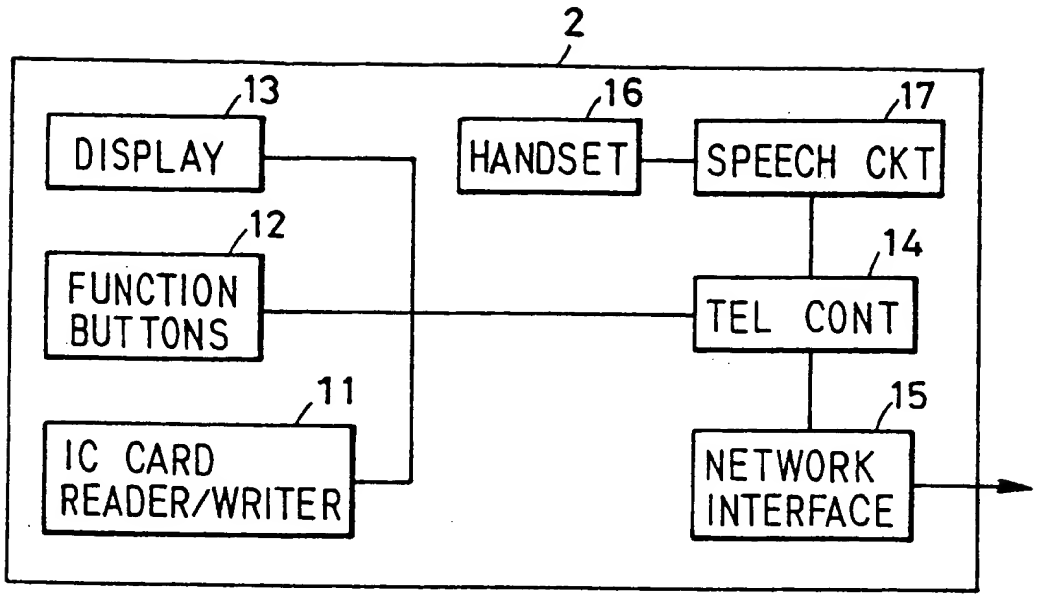

2
13
DISPLAY
16
HANDSET
17
SPEECH CKT
12
FUNCTION BUTTONS
14
TEL CONT
11
IC CARD READER/WRITER
15
NETWORK INTERFACE

FIG. 3

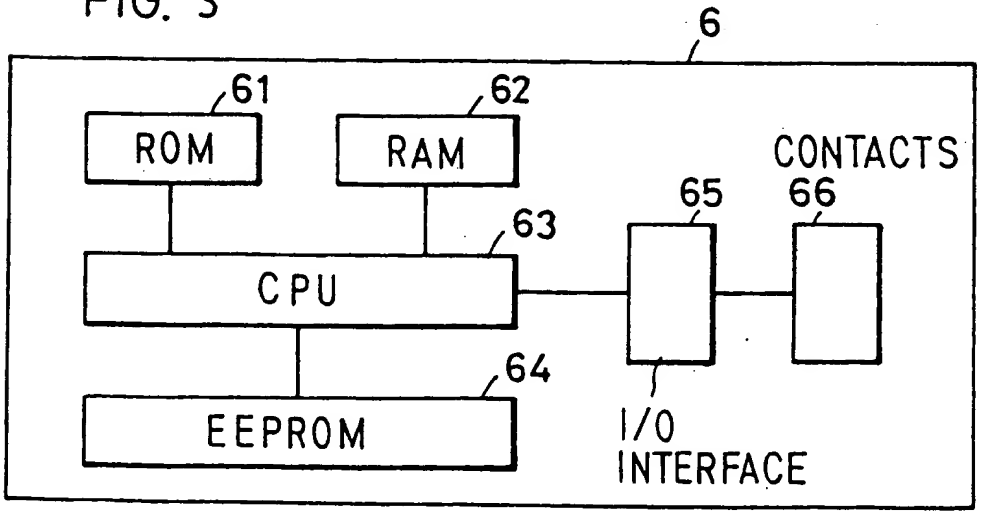

6
61
ROM
62
RAM
CONTACTS
65
66
63
CPU
64
EEPROM
I/O INTERFACE

FIG. 5

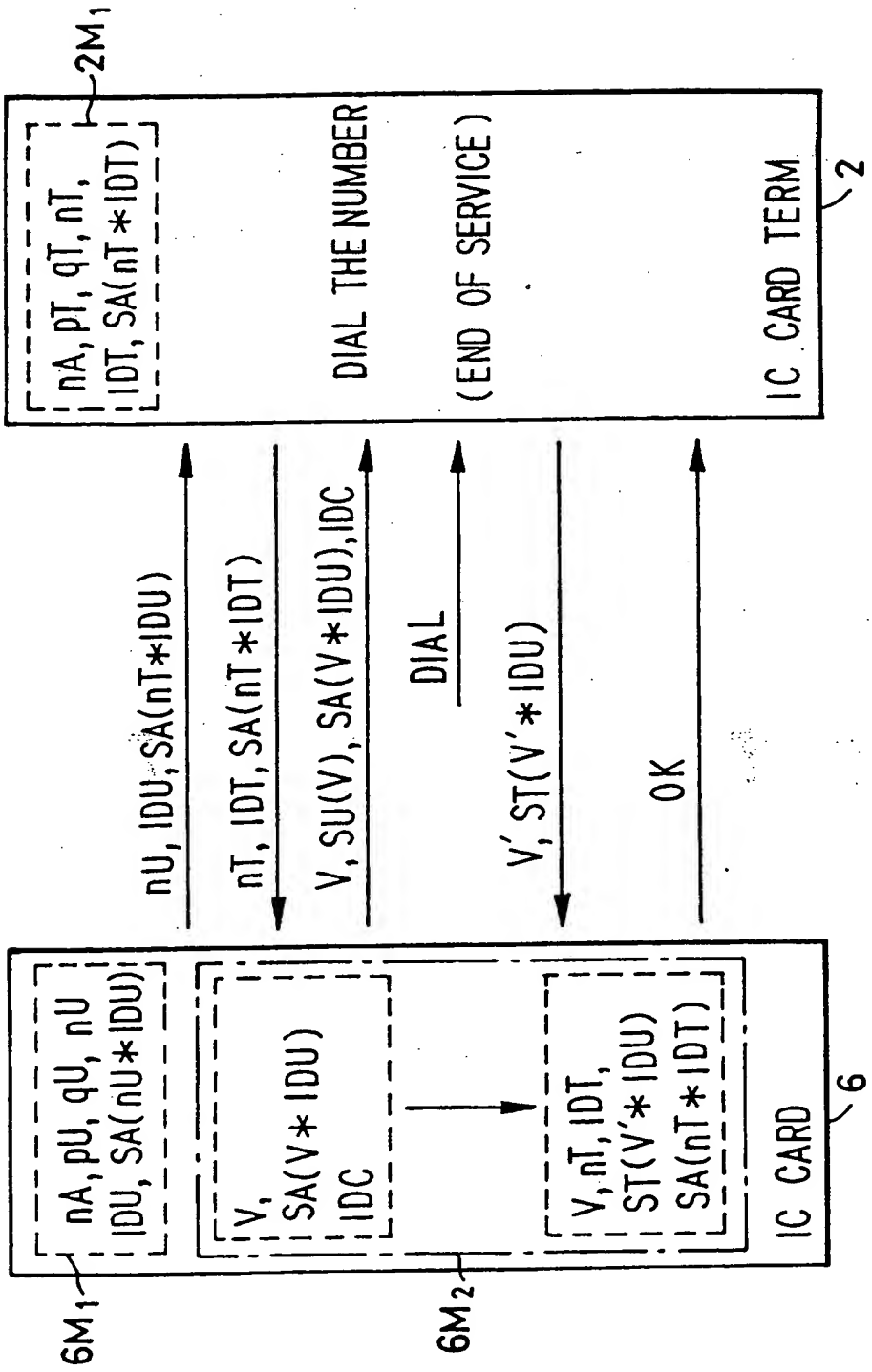

2M1
nA, pT, qT, nT,
IDT, SA(nT*IDT)
DIAL THE NUMBER
(END OF SERVICE)
IC CARD TERM
2
nU, IDU, SA(nT*IDU)
nT, IDT, SA(nT*IDT)
V, SU(V), SA(V*IDU), IDC
DIAL
V', ST(V'*IDU)
OK
6M1
nA, pU, qU, nU
IDU, SA(nU*IDU)
V,
SA(V*IDU)
IDC
6M2
V, nT, IDT,
ST(V'*IDU)
SA(nT*IDT)
IC CARD
6

FIG. 6

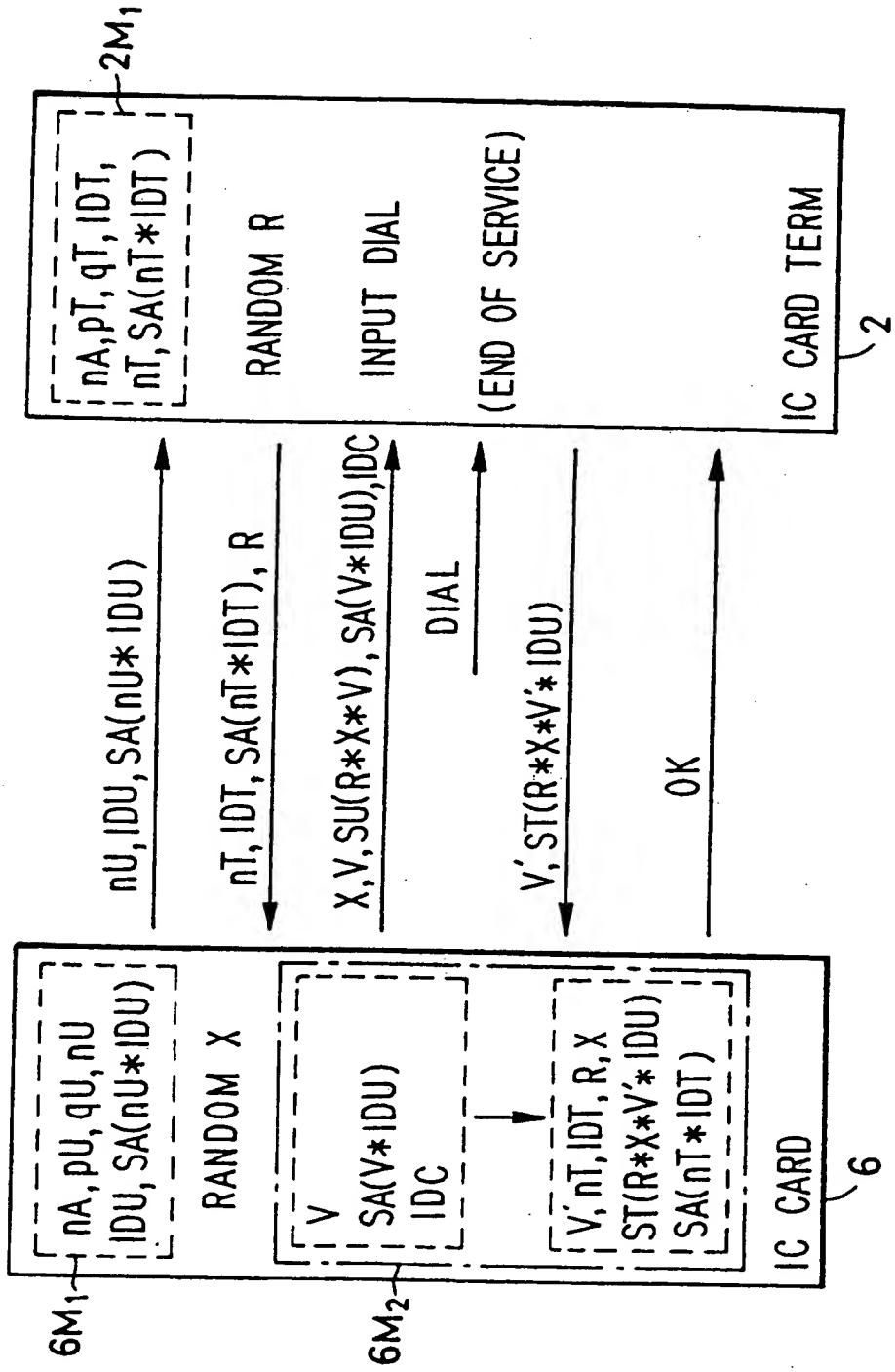

2M1
nA, pT, qT, IDT,
nT, SA(nT*IDT)
RANDOM R
INPUT DIAL
(END OF SERVICE)
IC CARD TERM
2
nU, IDU, SA(nU* IDU)
nT, IDT, SA(nT*IDT), R
X, V, SU(R*X*V), SA(V*IDU), IDC
DIAL
V', ST(R*X*V'* IDU)
OK
6M1
nA, pU, qU, nU
IDU, SA(nU*IDU)
RANDOM X
6M2
V
SA(V*IDU)
IDC
V', nT, IDT, R, X
ST(R*X*V'* IDU)
SA(nT*IDT)
IC CARD
6

FIG. 8

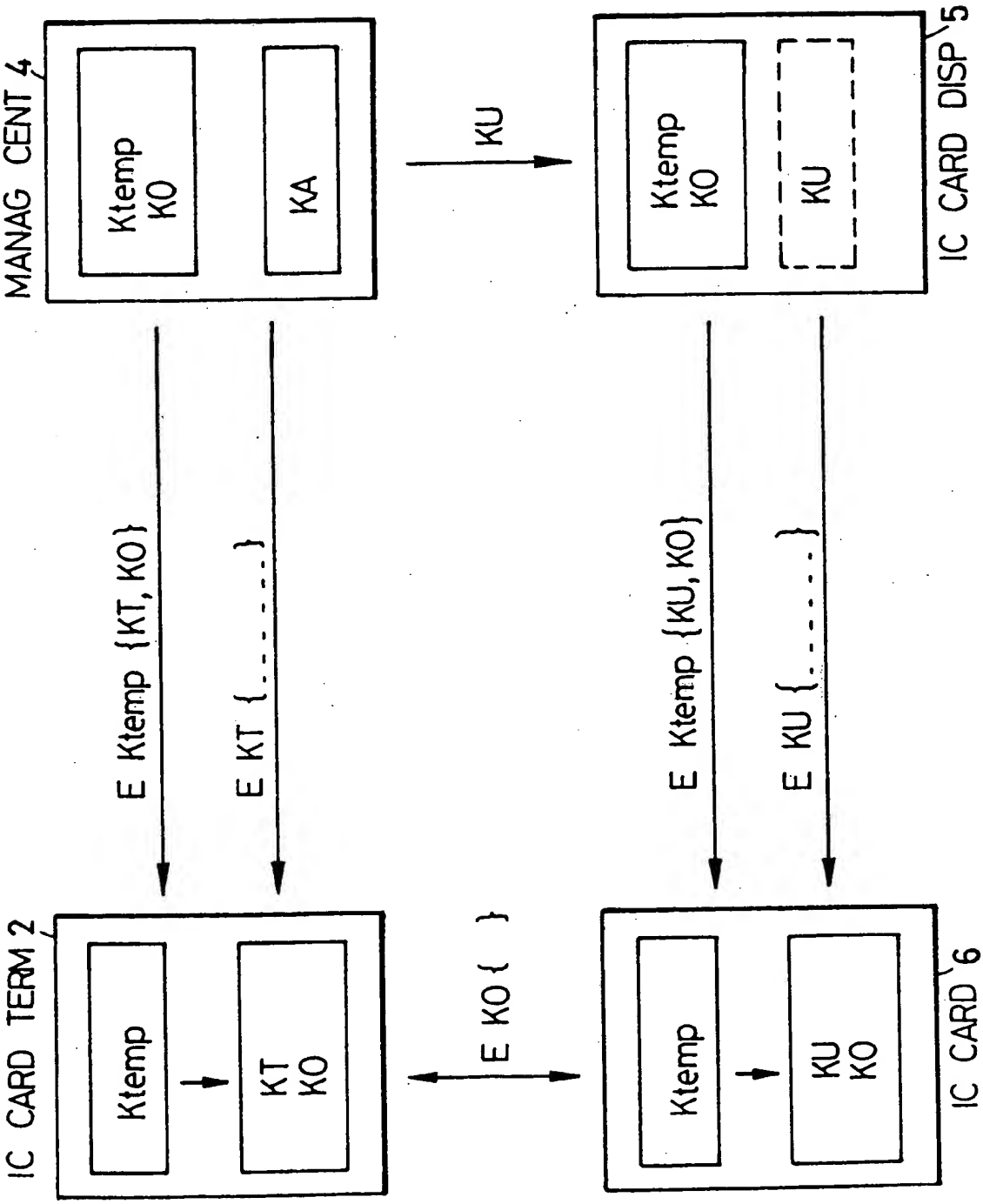

MANAG CENT 4
Ktemp KO
KA
KU
IC CARD DISP 5
Ktemp KO
KU
E Ktemp {KT, KO}
E KT {.....}
E Ktemp {KU, KO}
E KU {.....}
IC CARD TERM 2
Ktemp
KT KO
E KO { }
Ktemp
KU KO
IC CARD 6

FIG. 10

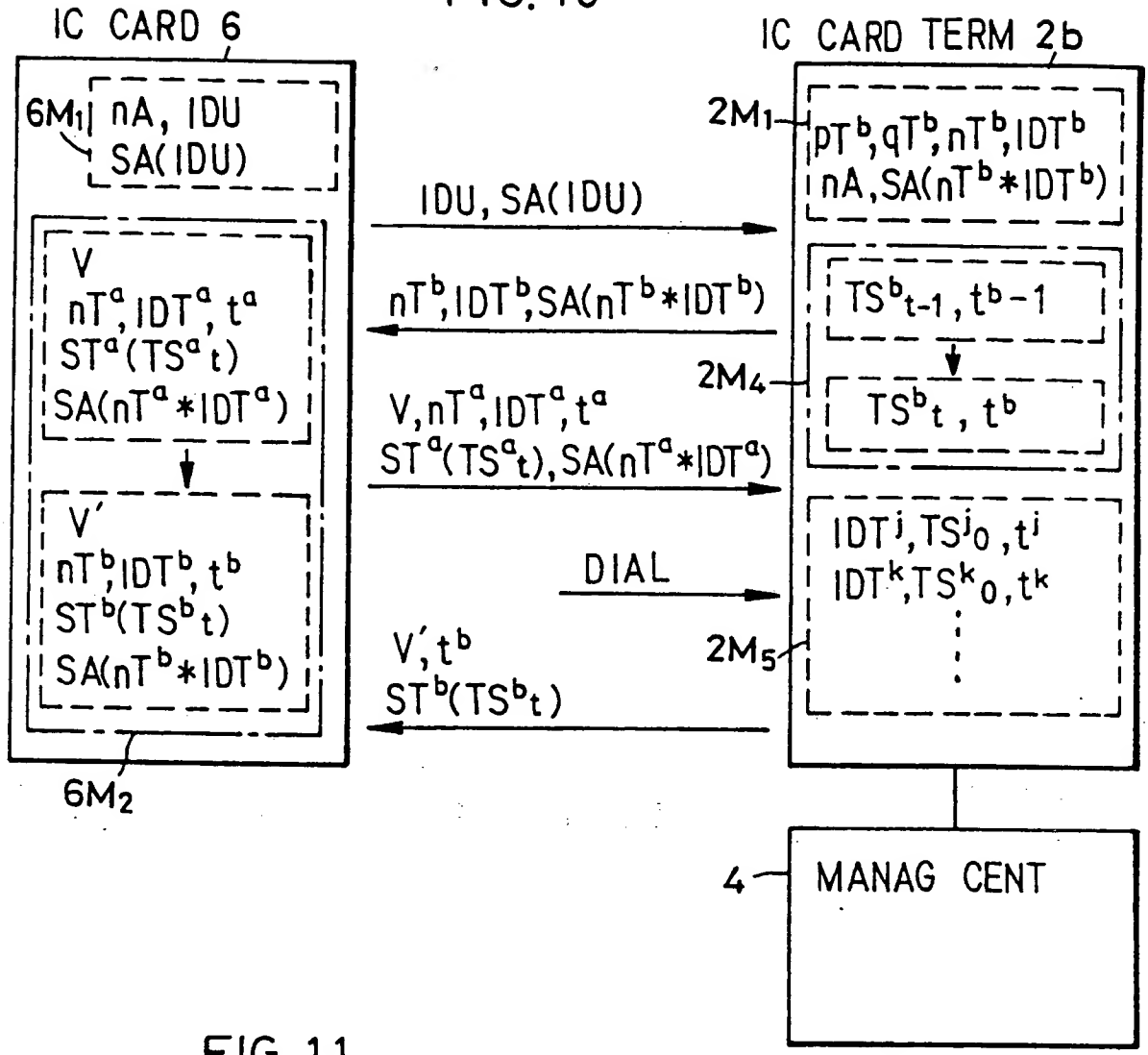

IC CARD 6
IC CARD TERM 2b
6M1
nA, IDU
SA(IDU)
IDU, SA(IDU)
2M1
pT^b, qT^b, nT^b, IDT^b
nA, SA(nT^b * IDT^b)
V
nT^a, IDT^a, t^a
ST^a(TS^a t)
SA(nT^a * IDT^a)
nT^b, IDT^b, SA(nT^b * IDT^b)
TS^b t-1, t^b - 1
2M4
TS^b t, t^b
V, nT^a, IDT^a, t^a
ST^a(TS^a t), SA(nT^a * IDT^a)
V'
nT^b, IDT^b, t^b
ST^b(TS^b t)
SA(nT^b * IDT^b)
DIAL
IDT^j, TS^j 0, t^j
IDT^k, TS^k 0, t^k
V', t^b
ST^b(TS^b t)
2M5
6M2
4
MANAG CENT

FIG. 11

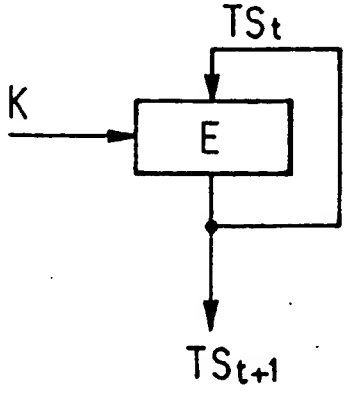

TSt
K
E
TSt+1

FIG. 13

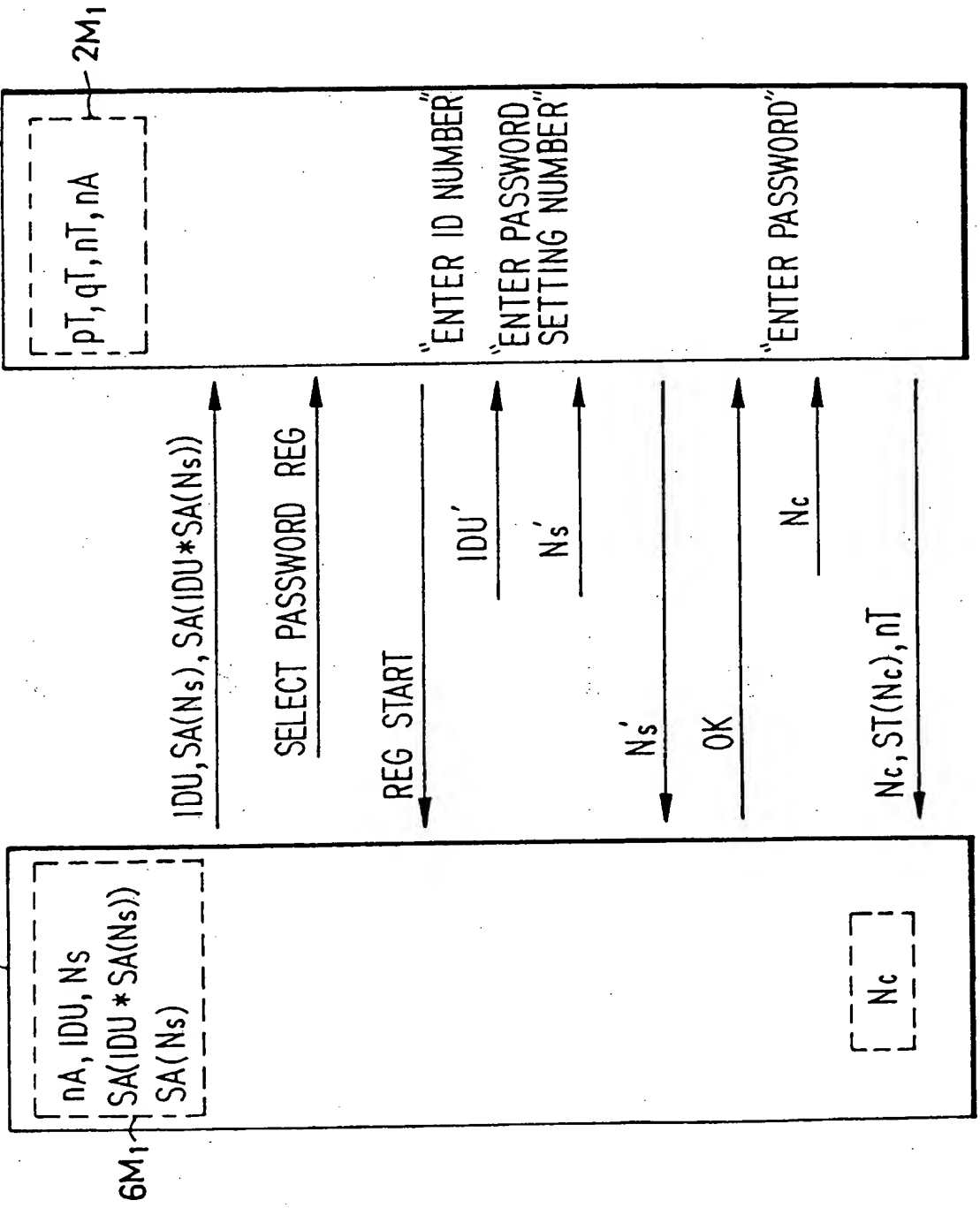

IC CARD TERM 2
2M1
pT, qT, nT, nA
IC CARD 6
6M1
nA, IDU, Ns
SA(IDU * SA(Ns))
SA(Ns)
Nc
IDU, SA(Ns), SA(IDU*SA(Ns))
SELECT PASSWORD REG
REG START
IDU'
Ns'
Ns'
OK
Nc
Nc, ST(Nc), nT
"ENTER ID NUMBER"
"ENTER PASSWORD SETTING NUMBER"
"ENTER PASSWORD"

FIG. 15

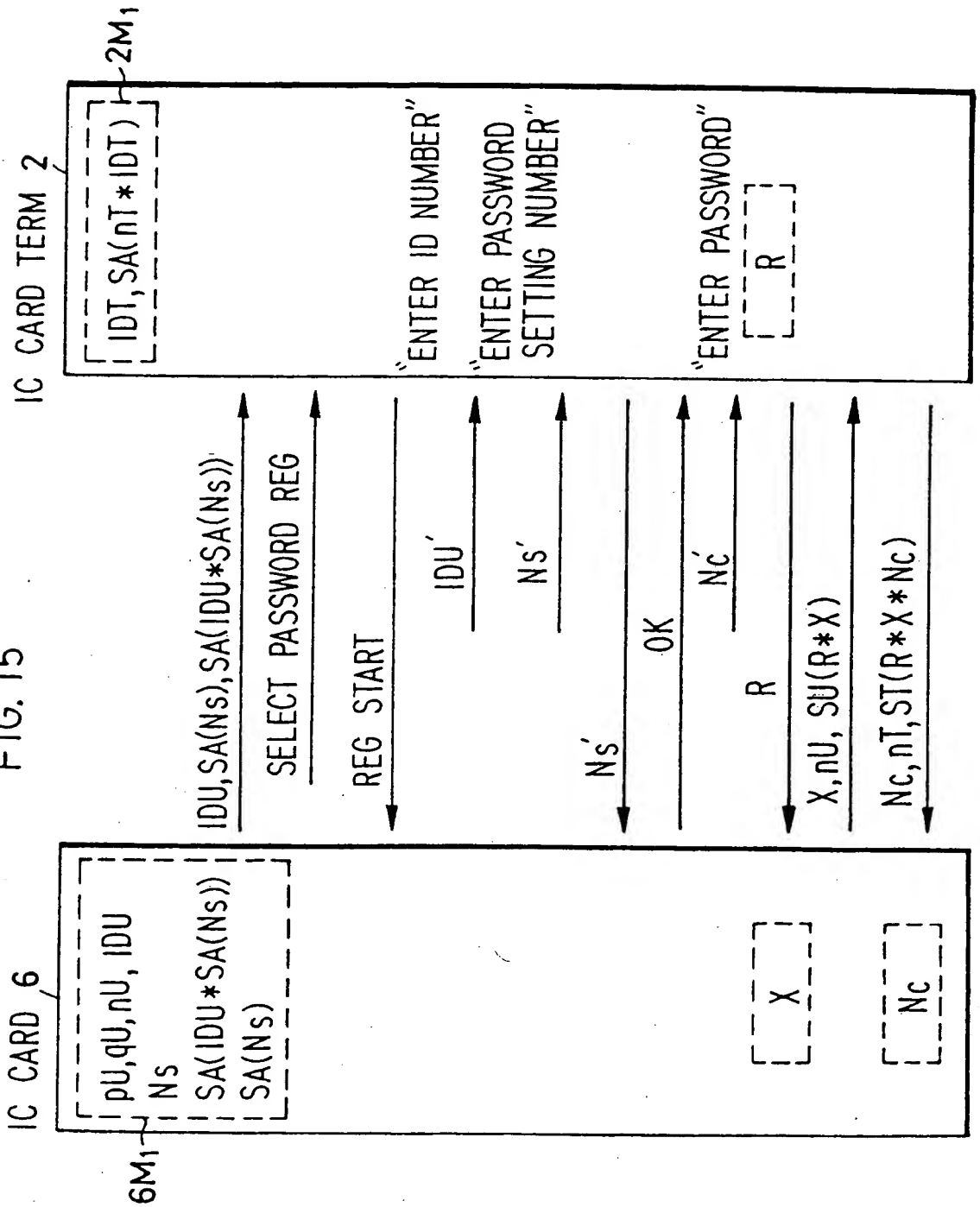
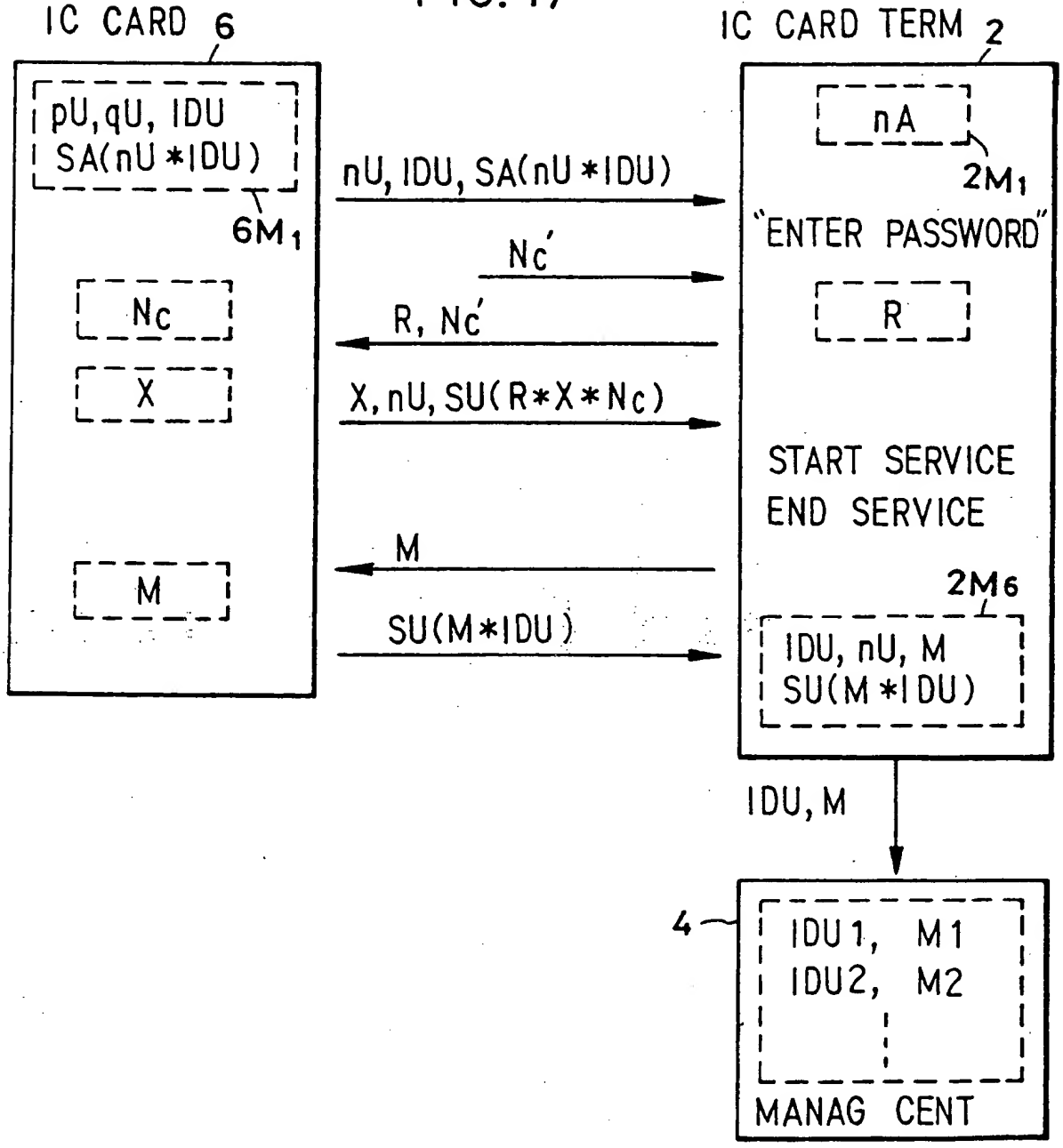

IC CARD 6
IC CARD TERM 2
2M1
6M1
pU, qU, nU, IDU
Ns
SA(IDU*SA(Ns))
SA(Ns)
IDT, SA(nT*IDT)
IDU, SA(Ns), SA(IDU*SA(Ns))
SELECT PASSWORD REG
REG START
"ENTER ID NUMBER"
IDU'
"ENTER PASSWORD SETTING NUMBER"
Ns'
Ns'
OK
"ENTER PASSWORD"
R
Nc'
R
X
X, nU, SU(R*X)
Nc
Nc, nT, ST(R*X*Nc)

FIG. 17


IC CARD 6
pU, qU, IDU
SA(nU*IDU)
6M1
Nc
X
M
IC CARD TERM 2
nA
2M1
"ENTER PASSWORD"
R
START SERVICE
END SERVICE
2M6
IDU, nU, M
SU(M*IDU)
nU, IDU, SA(nU*IDU)
Nc'
R, Nc'
X, nU, SU(R*X*Nc)
M
SU(M*IDU)
IDU, M
4
IDU1, M1
IDU2, M2
MANAG CENT

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 588 339 A3**

(12) # EUROPEAN PATENT APPLICATION

(21) Application number: **93114917.3**

(51) Int. Cl.[6]: **G07F 7/10**, G06F 15/00

(22) Date of filing: **16.09.93**

(30) Priority: **18.09.92 JP 249293/92**
18.09.92 JP 249294/92
18.11.92 JP 308688/92
26.11.92 JP 317254/92
26.11.92 JP 317255/92

(43) Date of publication of application:
23.03.94 Bulletin 94/12

(84) Designated Contracting States:
DE FR GB

(88) Date of deferred publication of the search report:
24.05.95 Bulletin 95/21

(71) Applicant: **NIPPON TELEGRAPH AND TELEPHONE CORPORATION**
1-6 Uchisaiwaicho 1-chome
Chiyoda-ku
Tokyo (JP)

(72) Inventor: **Ishiguro, Ginya**
Gurin Haitsu 12-2-403,
580, Nagasawa
Yokosuka-shi,
Kanagawa (JP)
Inventor: **Muta, Toshiyasu**
1927, Nagasawa
Yokosuka-shi,
Kanagawa (JP)
Inventor: **Sakita, Kazutaka**
2-14-1-613, Kaneya
Yokosuka-shi,
Kanagawa (JP)
Inventor: **Miyaguchi, Shoji**
5-20-19, Bessho,
Ninami-ku
Yokohama-shi,
Kanagawa (JP)
Inventor: **Okamoto, Tatsuaki**
94-2-5-503, Nagasawa
Yokosuka-shi,
Kanagawa (JP)
Inventor: **Fujioka, Atsushi**
B-305, 9-2-12, Sugita,
Isogo-ku
Yokohama-shi,
Kanagawa (JP)

(74) Representative: **Hoffmann, Eckart, Dipl.-Ing.**
Patentanwalt
Bahnhofstrasse 103
D-82166 Gräfelfing (DE)

(54) **Method and apparatus for settlement of accounts by IC cards.**

(57) An IC card (6) has a card information memory area wherein there are written a master public key nA, card secret keys pU and qU, a card public key nU, a card identification number IDU, and a first master digital signature SA1 for information including the card identification number. An IC card terminal (2a,2b) has terminal information memory area wherein there are written a master public key nA, terminal secret keys pT and qT, a terminal public key nT, a terminal identification number IDT, and a second master digital signature SA2 for information including the terminal identification number IDT. When inserted into the IC card terminal, the IC card sends thereto the data nU, IDU, and SA1. The IC card terminal verifies the digital signature SA1 by the master public key nA and, if it is valid, transmits the data nT, IDT and SA2 to the IC card. The IC card verifies the digital signature SA2 by the master public key nA and, if it is valid, transmits information corresponding to the current remainder value V to the IC card terminal. The IC card terminal makes a check to see if the received information corresponding to the remainder value V is appropriate, and if so, becomes enabled for providing a service.

EP 0 588 339 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 93 11 4917

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
A	EP-A-0 064 779 (SVENSKA PHILIPSFORETAGEN) * abstract; claims 1,2 *	1,10,13, 15, 17-20, 22-26	
A	EP-A-0 082 958 (IBM) * abstract; claim 1 *	1,10,13, 15, 17-20, 22-26	
A	EP-A-0 422 230 (MATSUSHITA) * abstract *	1,10,13, 15, 17-20, 22-26	
A	EP-A-0 281 059 (SIEMENS) * abstract *	1,10,13, 15, 17-20, 22-26	

TECHNICAL FIELDS SEARCHED (Int.Cl.5)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	14 February 1995	Taccoen, J-F

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirement of unity of invention and relates to several inventions or groups of inventions, namely:

1. Claims 1-9,15,16: Settlement of charges
2. Claims 10-12 : Creating of IC card
3. Claims 13,14 : Password registration
4. Claims 17,19, 22,25 : IC card terminal
5. Claim 18 : IC card
6. Claims 20,23,24, 26,27 : IC card system